

Symantec™ Messaging Gateway 9.5 Command Line Reference Guide

powered by Brightmail™



The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version: 9.5.0

Legal Notice

Copyright © 2011 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo, Brightmail™, the Brightmail™ logo, BLOC, BrightSig, The Anti-Spam Leader, Probe Network, and Norton Anti-Virus are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This Symantec product may contain third party software for which Symantec is required to provide attribution to the third party ("Third Party Programs"). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Please see the Third Party Legal Notice Appendix to this Documentation or TPIP ReadMe File accompanying this Symantec product for more information on the Third Party Programs.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043
<http://www.symantec.com>

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our Web site at the following URL:

www.symantec.com/business/support/

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level

- Hardware information
- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
 - Error messages and log files
 - Troubleshooting that was performed before contacting Symantec
 - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs or manuals

Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan	customercare_apac@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Command reference

This document includes the following topics:

- [Administering Symantec Messaging Gateway through the command line](#)
- [Command line interface access methods](#)
- [agent-config](#)
- [cat](#)
- [cc-config](#)
- [clear](#)
- [db-backup](#)
- [db-restore](#)
- [delete](#)
- [diagnostics](#)
- [dns-control](#)
- [grep](#)
- [help](#)
- [ifconfig](#)
- [iostat](#)
- [ldapsearch](#)
- [list](#)
- [mallog](#)

- [malquery](#)
- [monitor](#)
- [more](#)
- [mta-control](#)
- [netstat](#)
- [nslookup](#)
- [password](#)
- [ping](#)
- [reboot](#)
- [route](#)
- [rpmdb](#)
- [service](#)
- [show](#)
- [shutdown](#)
- [sshd-config](#)
- [tail](#)
- [telnet](#)
- [traceroute](#)
- [update](#)

Administering Symantec Messaging Gateway through the command line

Each appliance (physical or virtual) has a set of commands that you can use to configure, optimize, and administer your product. You can execute these commands from an SSH session or from the system console. The help for these commands is presented in Linux man page format.

See “[Command line interface access methods](#)” on page 11.

These help pages use the following Linux man page conventions:

- Square brackets ([]) indicate that a statement is optional
- The pipe character (|) indicates that one of two statements can be specified
- Text in *italics* indicates that the text should be replaced with the text that you specify

The Symantec Messaging Gateway man pages contain the following sections:

- Synopsis
A description of the options and arguments available for the command.
- Description
General information about the command.
- Options
Options that you can use to control the behavior of a command. Options always begin with one or two dashes, such as `-s` or `--status`. Use two dashes for the full term; one dash for the abbreviated term.
Some options have arguments. For example, `--log level`. Square brackets mean that element of the command is optional.
Not all commands have options.
- Arguments
Some commands require arguments. Arguments are names of files, host names, IP addresses, and so on that you specify to control the behavior of the command. Not all commands have arguments. Unlike options, you do not precede arguments with dashes.
- Examples
This section provides sample command usage. Not all commands have examples.
- See Also
This section lists related commands. Not all commands have see also references.

Use the following commands to navigate through the man pages:

- f or SPACE
Forward one window
- b
Backward one window
- /pattern
Search for a word or pattern
- <
Go to the beginning of the document
- >

Go to the end of the document

- q

Quit

- h

Display more help with man pages

Type `help command_name` to get information about a specific command. Type `help` to get general information about command-line man pages.

The following commands are available:

- `agent-config`
- `cat`
- `cc-config`
- `clear`
- `db-backup`
- `db-restore`
- `delete`
- `diagnostics`
- `dns-control`
- `grep`
- `help`
- `ifconfig`
- `iostat`
- `ldapsearch`
- `list`
- `mallog`
- `malquery`
- `monitor`
- `more`
- `mta-control`
- `netstat`
- `nslookup`

- [password](#)
- [ping](#)
- [reboot](#)
- [route](#)
- [rpmdb](#)
- [service](#)
- [show](#)
- [shutdown](#)
- [sshd-config](#)
- [tail](#)
- [telnet](#)
- [traceroute](#)
- [update](#)

Command line interface access methods

You can log into the command line interface on each Symantec Messaging Gateway appliance. Some of the commands duplicate functions in the Control Center. Some of the commands provide functions that are not available in the Control Center.

See “[Administering Symantec Messaging Gateway through the command line](#)” on page 8.

[Table A-1](#) and [Table A-2](#) describe the methods that you can use to access the command line interface. After connecting to the command line interface, type **admin** at the `login as:` prompt and type the administrator password at the `password:` prompt.

Table A-1 Command line interface access methods for physical appliances

Access method	How to connect
System console using directly attached keyboard and VGA monitor	<p>You must have physical access to the appliance to access the command line interface with a keyboard and VGA monitor.</p> <p>Connect a keyboard to the keyboard port on the appliance. Connect a VGA-compatible monitor to the D-sub 15 VGA port on the appliance.</p> <p>You can also connect the keyboard and VGA ports on the appliance to a KVM switch.</p>
System console using a serial cable	<p>You must have physical access to the appliance to access the command line interface with serial cable.</p> <p>Connect a null modem cable from the DB9 serial port on the appliance to the serial port on another computer. Use a terminal emulation software on the computer to access the appliance through the serial port. On a Windows computer, ensure that the terminal emulation software is set to use the correct COM port. Configure the terminal emulation software on the computer to the following settings:</p> <ul style="list-style-type: none"> ■ 9600 bps ■ 8 data bits ■ No parity bit ■ 1 stop bit
Remote access using an SSH client	<p>Using an SSH client lets you access the command line interface from any computer on your network, unless firewall rules prohibit access.</p> <p>For a Windows computer, use an SSH client such as PuTTY. On a UNIX computer you can use the <code>ssh</code> command that is typically included in the operating system.</p> <p>The host name or IP address to connect to using the SSH client is the name you specified when you initially configured the appliance. For a Control Center appliance, the host name is also the name in the URL that you use to access the Control Center.</p>

Table A-2 Command line interface access methods for virtual appliances

Access method	How to connect
VMware Virtual Machine Console	<p>You can use the VMware Virtual Machine Console to log into the virtual appliance. Refer to the VMware Virtual Machine Console documentation for more information.</p>

Table A-2

Command line interface access methods for virtual appliances

(continued)

Access method	How to connect
Remote access using an SSH client	<p>If you configured the virtual appliance with a host name or IP address that resolves on your network, you can use an SSH client to access the command line interface. You can access the virtual appliance from any computer on your network, unless firewall rules prohibit access.</p> <p>For a Windows computer, use an SSH client such as PuTTY. On a UNIX computer you can use the <code>ssh</code> command that is typically included in the operating system.</p>

agent-config

`agent-config` – configures the agent that connects hosts to the Control Center

SYNOPSIS

```
agent-config [--norestart] [--force] --add | --delete ip
agent-config --help | --status
agent-config [--norestart] --log level
```

DESCRIPTION

The `agent-config` command lets you edit the allowed IP configuration for the Scanner. Use this command when you change the IP address of the Control Center. You must run this command on every host to re-allow the new Control Center IP to connect to the hosts. The Agent restarts when you add or delete an IP address to or from the allowed IP list, unless you include `--norestart` in the command.

OPTIONS

`--add, -a ip`

Add an IP address to the agent-allowed IP address list. Specify an IP address in dotted quad format. For example, `192.168.2.1`.

`--delete, -d ip`

Delete an IP address from the agent-allowed IP address list. Specify an IP address in dotted quad format. For example, `192.168.2.1`.

`--log, -l level`

Set the log level. The log levels are listed below from least verbose to most verbose and each level includes the previous level. For example, if you specify the `errors` level, only the most urgent log messages are stored. If you specify the `notices` level, `errors`, `warnings`, and `notices` level log messages are stored.

Specify one of the following log levels:

- `errors`
- `warnings`
- `notices`
- `information`
- `debug`

`--force, -f`

Used with `--delete` option to bypass the deletion warning.

`--help, -h`

Display this message.

`--norestart, -n`

Do not restart the agent after modifying the IP address list or log level.

`--status, -s`

Display the allowed IP address list and current log level.

cat

`cat` – standard Linux command to view a file

DESCRIPTION

The `cat` command displays the contents of plain text files. The `more` command can be more useful than `cat` for listing long files or multiple files.

Type `help cat` on the command line for more information about the options available for `cat`. The information that is displayed may contain references to commands that are not available on Symantec Messaging Gateway.

The `cat` command is a standard Linux command that has been modified to only display the files that the `list` command shows.

SEE ALSO

See [list](#) on page 51.

See [more](#) on page 66.

cc-config

`cc-config` – configures the logging and network access to the Control Center

SYNOPSIS

```
cc-config ( --help | --status )
cc-config cclog --level level
cc-config compliancelog --days days
cc-config database ( --status | --check [tableName] | --repair
[tableName] | --optimize [tableName] )
cc-config http ( --on | --off )
cc-config port-443 ( --on | --off )
```

DESCRIPTION

The `cc-config` command lets you modify the selected settings that the Control Center uses. These settings include Content Filtering Audit logs, port 443 access, and more.

ARGUMENTS

`cclog`

Change the log level of the main Control Center log, BrightmailLog.log.

When you apply this to the Control Center log, `cc-config` writes the command-line parameters to the log4j properties file. It then restarts the Control Center.

`compliancelog`

Change the rollover frequency of the Content Filtering log.

`database`

List, optimize, validate, or repair the database tables that the Control Center uses.

Ensure that you validate the database using the `cc-config database --check` command before updating your Symantec Messaging Gateway. If there are any errors in the tables, repair the erroneous tables using `cc-config database --repair [tableName]` command and then update your Symantec Messaging Gateway.

`http`

Turn on or off access to the Control Center using HTTP and port 41080.

If http access is off, you cannot access the Control Center with a URL that starts with `http://`. If http access is on, you can access the Control Center with a URL that starts with `http://`. To access the Control Center using http, append `:41080` to the URL. Regardless of the http setting, you can always access the Control Center with a URL that starts with `https://`. Unlike HTTPS, HTTP is not a secure protocol, so the communication between your Web browser and the Control Center could be monitored by a third party.

`port-443`

Turn on or off access to the Control Center using HTTPS and port 443 (the standard, SSL-secured port for Web servers).

When port 443 access is off, you must append `:41443` to the URL when you use an `https://` URL to access the Control Center. When port 443 access is enabled, you do not need to append the port number for an `https://` URL to access the Control Center.

OPTIONS

`--check, -c`

Check the given database table. If no table name is specified, then check all tables.

`--days, -d`

Set the number of days to keep logs before they roll over.

`--help, -h`

Display this message.

`--level, -l`

Set the log level. The log levels are listed below from least verbose to most verbose and each level includes the previous level. For example, if you specify the `errors` level, only the most urgent log messages are stored. If you specify the `debug` level, `errors`, `warnings`, `information` and `debug` level log messages are stored.

Specify one of the following log levels:

- `errors`
- `warnings`
- `information`
- `debug`

`--off`

Disable a feature.

`--on`

Enable a feature.

`--optimize, -o`

Optimize the table so it takes less space on disk. If no table name is specified, then optimize all tables.

`--repair, -r`

Repair the given database table. If no table name is specified, then attempt a repair operation on all damaged tables.

`--status, -s`

Display the current log settings and port statuses.

clear

`clear` – standard Linux command to clear the screen

SYNOPSIS

`clear`

DESCRIPTION

The `clear` command erases all of the text on the screen and displays the command prompt at the top of the screen.

This command is a standard Linux command that has not been modified.

db-backup

db-backup – back up the Control Center database

SYNOPSIS

db-backup [options]

DESCRIPTION

The `db-backup` command backs up the Brightmail databases, such as configuration settings, report data, log data, and incidents. You can store backups on the appliance or on a remote server. Only run this command on the appliance that contains the Control Center. This command does not function on a Scanner-only appliance. Only one instance of `db-backup` can run at a time.

By default, backup files are compressed before they are written to disk to minimize the size of backup files. The `db-backup` command calculates the amount of disk space the backup file requires. The command does not run unless at least twice this amount is available on the `/data` partition.

Use `db-restore` or the Control Center restore feature to restore a backup on the appliance or a backup on a remote computer. If you specify `--file path` for a backup to the appliance, you can only restore the backup using the `db-restore` command, not the Control Center restore feature.

You can also create backups using the Control Center. In the Control Center, click **Administration > Hosts > Version > Backup**.

OPTIONS

`--backup, -b number`

The number of backups to store on the appliance. If you have more backups stored than *number*, then older backups are deleted. Each unique combination of type and schedule is retained separately. If you do not specify `--backup number`, the default is 5 for each type and schedule combination. See examples 4 and 6.

`--file, -f path`

The name and, optionally, location to save the backup. Use the `--file` option to specify an alternate file name for the backup file or to save the backup file to a remote computer. If you do not specify `--file path`, the backup is saved to the appliance as

`db-backup.brightmail.Mon-Day-Year-Hour-Min.full.manual.tar.bz2`.

You can save the backup to a remote computer using either FTP (file transfer protocol) or SCP (secure copy protocol). If the path ends with / the backup is saved in that directory using the default file name. If the path ends with a file name the backup is saved with that name in the specified path. When you save the backup to a remote computer, `db-backup` temporarily stores the backup file on the appliance, checks the file for data integrity, copies the file to the remote computer, and checks to ensure that the file was successfully copied.

Use one of the following two path formats to save the backup to a remote server:

FTP

Use the following format: `ftp://'user': 'password'@host[:port]/path`. If special characters are included in the password, you must enclose the password in single quotes ('). If the special characters in a password include a single quote, you can use the double quote instead ("). Passwords containing single and double quotes are not valid. If no user name and password are specified, an anonymous login is used.

SCP

Use the following format: `scp://'user'@host/path`. You must specify a user name. The `db-backup` command prompts you for the password.

`--gzip, -g`

Use the gzip compression algorithm instead of the default bzip2 compression algorithm. The gzip algorithm performs less efficient compression than bzip2.

`--list, -l`

List existing backups on the appliance.

`--help, -h`

Display this message.

`--nocompress, -n`

Do not compress the backup file. Use this option if you want to visually scan the file contents.

`--purge, -p`

Purge backups. Use the `--purge` option to delete old backup files that match the parameters that you specify. To delete all but the *number* most recent backups of a type and schedule combination, specify `--purge --backup number` along with the type and schedule. Specify `--purge --backup 0` to delete all backups of a type and schedule combination. To delete a specific file, specify `--file file` along with `--purge`. See examples 5 and 6.

`--schedule, -s schedule`

The schedule name to include in the backup file name. If you specify a schedule name, `db-backup` does not create automatic backups at that interval. The schedule that you specify only names the backup file with that name. The schedule names differentiate backups. See `--backup` and `--purge` for more information. Use the backup feature in the Control Center to create automatic scheduled backups. The following schedules are available:

`manual`

Label this backup a manual backup. This option is the default.

`daily`

Label the backup a daily, manual backup.

`weekly`

Label the backup a weekly, manual backup.

`monthly`

Label the backup a monthly, manual backup.

`--type, -t type`

The type of backup to create. Each backup type has two aliases that are alternate short versions of the backup type. See example 4. The following types are available:

`full`

Perform a full backup (aliases: `f`, `1`). This option is the default.

`config-incidents`

Back up configuration and content filtering incident data (aliases: `ci`, `2`).

`config-incidents-reports-logs`

Back up configuration, content filtering incident, report and log data (aliases: `cirl`, `3`).

EXAMPLES

Example 1

Save a full backup on the appliance with the default schedule of `manual` and the default type of `full`. The newest five backups with a schedule of `manual` and type of `full` are kept (including the backup just created) and the rest of the backups matching that combination are deleted.

`db-backup`

Example 2

Save a full backup on a remote server with SCP. The database backup file in the format `db-backup.brightmail.date-time.full.manual.tar.bz2` is copied to 192.168.2.42 in the `/tmp` directory through SCP. Log on to the SCP server with the `support` user account. The `db-backup` command prompts for the password for the `support` user account.

```
db-backup --file scp://support@192.168.2.42/tmp/
```

Example 3

Save a full backup on a remote server with FTP. The database backup file `db-backup.brightmail.date-time.full.manual.tar.bz2` is copied to `host.symantecexample.org` in the `/user/jmuir` directory. Log on to the FTP server with the `jmuir` user account and `secret` password.

```
db-backup -f ftp://jmuir:secret@host.symantecexample.org/user/jmuir/
```

Example 4

Backup configuration and content filtering incident data to the appliance and include the word `weekly` in the backup file name. In addition to the newly created backup, keep one additional existing backup with `config-incidents` and `weekly` in the file name.

```
db-backup --backup 2 --schedule weekly --type ci
```

Example 5

Delete a single backup file.

```
db-backup --purge --file  
db-backup.brightmail.Jan-21-10-19-26.config-incidents.weekly.tar.bz2
```

Example 6

Delete all but the one most recent backup file of type `config-incidents` and schedule `manual`.

```
db-backup --purge --backup 1 --type config-incidents --schedule manual
```

SEE ALSO

See [db-restore](#) on page 25.

db-restore

`db-restore` - restores the brightmail databases to an appliance from previously created backups on the appliance or from remote locations with FTP and SCP.

SYNOPSIS

```
db-restore [--force --list --help] file
```

DESCRIPTION

The `db-restore` command restores brightmail databases to an appliance from a single, previously created backup. These are the backups that you have previously generated and saved on the appliance or from remote locations with FTP and SCP. If you attempt to run more than one instance of `db-restore` at a time, an error results. If any part of the operation fails, `db-restore` fails, and an explanatory message appears on the command line. You must be on the Control Center host to use the `db-restore` command.

Note: Restoring an appliance immediately after resetting the appliance to its factory default might leave the appliance in an unusable state. Therefore, you must complete the site setup before restoring an appliance that is reset to its factory default.

When you restore a database backup on a different appliance than it was created, keep in mind the following considerations:

- If you restore the appliance from a backup taken on a different appliance, the restored appliance does not affect the configuration settings on the new host. However, the virtual IP addresses are not created during the configuration. Virtual IPs defined in the old Control Center host are mapped by default to an interface on the new Control Center host. You can avoid the mapping of virtual IPs from the old Control Center host to the interface on the new Control Center host by completing the site setup. Alternatively, you can create the virtual IPs on the new Control Center host after the restore.
- If you attempt to restore a backup to an appliance other than the one on which it was created, you must reboot the appliance.

Stop the Control Center while this operation runs. Restart it when the restore has completed.

OPTIONS

`--force, -f`

Force a restore even when the version of appliance software in the backup file differs from the software that is currently on the appliance.

`--list, -l`

List the backup files that are stored on the appliance.

`--help, -h`

Display this message.

ARGUMENTS

Specify *file* with one of the following formats. If the file is stored on a remote computer, specify the directory path to the file.

file

Type the file name without the FTP or SCP prefix to specify a backup that is stored locally.

`ftp://user:password[:port] /path`

Copy files from their remote location with FTP.

Logon is attempted with the user name and password credentials that you provide on the command line. If special characters are included in the password, enclose the password in single quotes ('). If the special characters in a password include a single quote, you can use the double quote instead ("). If no credentials are specified, anonymous logon is used. Error checking ensures that the copies are complete.

`scp://username@host/path`

Copy the backup file from its remote location with SCP. A complete path, file name, and user name are required when you specify a backup file through SCP. You are prompted for a password for the user name that you specify. Return codes are checked to ensure that the entire backup file is copied from the remote host. The script exits with non-zero status on failure. If the script fails, an error message appears. Error checking ensures that the copies are complete.

SEE ALSO

See [db-backup](#) on page 21.

See [diagnostics](#) on page 33.

delete

`delete` – clear logs, configuration information, and data

SYNOPSIS

```
delete [--purge num] component component ...  
delete file file
```

DESCRIPTION

Use the `delete` command to delete logs, configuration information, and other data. You may want to delete data if disk space is low or to clear configuration data to correct or diagnose a problem. The `delete` command restarts the Brightmail Engine if necessary after you run the `delete` command.

OPTIONS

`--purge`, `-p` *num*

Delete all database backup files except for the *num* most recent files. This option is only valid with the `database` component.

ARGUMENTS

You can delete individual files or you can specify one or more components to delete logical groups of files.

`file` *file*

Delete the file that you specify. You can only delete the files that you can view with the `list` command. Specify the entire path to the file as shown by the `list` command.

Symantec recommends that you delete items by specifying a component instead of deleting individual files. If you delete individual files, you may change the effectiveness or performance of Symantec Messaging Gateway. If you delete log files or temporary files with the `delete file file` command, some log data may be lost. To delete log files, specify one of the components in the log components group.

If you do delete individual log files with the `delete file file` command, restart the service that applies to the log file that you deleted. For example, if you delete the Control Center log file `Brightmaillog.log`, restart the Control

Center service. Use the `service` command or the Control Center to restart a service.

The following components are available and are listed in groups of similar behavior.

Log components:

`alllogs`

Delete all logs in the log component group.

`bcclogs`

Delete all Control Center logs.

`ddslogs`

Delete all directory data service logs.

If you delete `ddslogs`, the `bmclient_log` and `bmserver_log` log files may contain many `Could not connect: Connection refused` errors. These errors are normal.

`imlogs`

Delete all IM logs.

`mallogs`

Delete all Message Audit Logs.

`oslogs`

Delete all operating system logs.

`scannerlogs`

Delete all Scanner logs.

Configuration components:

`allconfig`

Delete all configuration data in the configuration component group.

`bccconfig`

Delete all Control Center configuration files.

`clearsockets`

Delete all socket files in the `/var/tmp` directory.

`ddsconfig`

Delete all directory data service configuration files.

`imconfig`

Delete IM configuration files.

osconfig

Delete operating system configuration files.

scannerconfig

Delete all of the Scanner configuration files for a given Scanner (including support sieve scripts). It does not affect the Scanner configuration information that is stored in the Control Center.

When you run `delete scannerconfig`, it restarts the appliance on which the command is run. After you run `delete scannerconfig`, you must recommit Scanner configuration information from the Control Center to disk and relicense your Scanner.

You can recommit the Scanner information to disk unchanged or edit the information to correct potential problems before you save this information to disk. To do either of these tasks, access **Administration > Hosts > Configuration** in the Control Center, select the Scanner, and click **Edit**. To recommit the information unchanged, click **Save**. Alternatively, edit any settings for this Scanner as necessary to correct a problem in the configuration and click **Save**.

You can delete the Scanner configuration if you change the Scanner configuration of an independent Scanner appliance. Then you can re-add it with the Add Scanner Wizard. This option is not available for an appliance that hosts both a Control Center and Scanner.

Symantec recommends that you do not use `delete scannerconfig`.

Data components:**alldata**

Delete all data in the data component group.

bccdata

Delete all Control Center data including any license files. Afterwards, your configuration is the same as an out-of-the-box the Control Center configuration.

ddsdata

Delete all directory data service data.

imdata

Delete all IM data.

keystore

Delete Control Center HTTPS certificates from the keystore.

scannerdata

Delete mail from MTA queues and the following file:

```
/data/scanner/rules/matchEngine/tmp/data_match_engine_jce_keystore
```

`spcdata`

Delete all Symantec Protection Center (SPC) data, and de-register any Symantec Messaging Gateway SPC instance. After using `spcdata`, you must re-register the Control Center with the SPC server in order to continue using the Control Center with SPC.

`sudata`

Delete all of the files that are related to software updates.

Quarantine components:

`allquarantine`

Delete all messages from all quarantines.

`contentquarantine`

Delete all content quarantine and informational messages.

`spamquarantine`

Delete all messages from Spam Quarantine.

`virusquarantine`

Delete all messages from Suspect Virus Quarantine.

Rule components:

`allrules`

Delete all rules and replace them with the factory default rules.

`avrules`

Delete all antivirus rules and replace them with the factory default rules.

`dayzerorules`

Delete all day zero rules and replace them with the factory defaults rules.

`fastpassrules`

Delete all Fastpass rules.

`gatekeeperrules`

Delete gatekeeper antispam rules and replace with factory default rules.

`intsigrules`

Delete all intsig rules and replace them with the factory default rules.

`ipfregrules`

Delete IP frequency rules.

`regexrules`

Delete regex filter rules.

spamhunterrules

Delete all spam hunter rules and replace them with the factory default rules.

spamsigrules

Delete spamsig rules and replace them with the factory default rules.

Note: The `delete` command may take half a minute to delete rules. Wait for the command prompt to return before you run additional commands. Do not press **Ctrl+C** to stop the `delete` command while it is running.

Miscellaneous components:

all

Delete all logs, configuration data, passwords, support sieve scripts, Scanner data, cores, diagnostic packages, rules, queue data, SPC data, and backup files to restore your appliance to the original factory configuration.

bcchostacl

Delete the Scanner access controls made on the **Administration > Settings > Control Center** page to permit access from all Scanners.

cores

Delete all core directories.

database

Delete all backups of the Control Center database that were created with `db-backup`.

diagnostics

Delete all diagnostic packages.

help

Display a summary of components that you can delete.

monitor

Delete the files made by the `monitor` command.

EXAMPLES

Example 1

Delete the `BrightmailLog.log` file.

```
delete file /data/logs/bcc/BrightmailLog.log
```

Example 2

Delete all messages in the Spam Quarantine.

```
delete spamquarantine
```

Example 3

Delete all Control Center database backup files that are stored on the appliance except for the three most recent backup files.

```
delete --purge 3 database
```

SEE ALSO

See [cat](#) on page 16.

See [list](#) on page 51.

See [more](#) on page 66.

diagnostics

diagnostics – generate diagnostics package

SYNOPSIS

```
diagnostics [options] url
```

DESCRIPTION

The `diagnostics` command generates a diagnostic package that Symantec Support can use to analyze problems with the product.

You should specify a valid URL unless you use the `--find-other-cores` option. If you specify a valid URL but do not specify the data collection options, `diagnostics` uses the following parameters by default:

```
--config --crash-info 5 --logs 100000
```

When the user name or password are part of the URL, write them in quotes if they have any special shell characters in them. The password can be specified in the URL or at the password prompt. An example of the URL syntax is as follows:

```
scp://'user':'password'\@host[:port]/path
```

If you specify a path that ends with a forward slash, the diagnostics file is written to the path that you specify with the default file name. If you specify a path that does not end with a forward slash, the backup file is written with the file name specified in the path.

The default diagnostics file name is in the following format:

```
diagnostics.yy-mm-dd-hh-mm.hostname.tar.gz
```

For example:

```
diagnostics.09-Sep-10-15-42.host9902.symantecexample.com.tar.gz
```

An option cannot be specified more than once whether it is in its long form or short form. For the `--cores` option, a component cannot be specified more than once either with the component name or convenient string `all`. If you attempt to, an error message appears along with the appropriate usage text.

OPTIONS

```
--config, -c
```

Collect only the configuration data. The configuration data includes Symantec Protection Center (SPC) registration details, if available.

`--cores, -o component n`

Collect the latest *n* core directories, including core files for a component. The valid range for *n* is 1 through 9,999.

The list of components include the following:

- `--cores mta n` collects MTA core packages
- `--cores bmagent n` collects Brightmail Agent core packages
- `--cores imrelay n` collects IM Relay core packages
- `--cores bmserver n` collects Brightmail Server core packages
- `--cores conduit n` collects Conduit core packages
- `--cores jlu-controller n` collects Java LiveUpdate core packages
- `--cores dds n` collects Directory Data Service core packages
- `--cores other n` collects the other core files that are not collected with other options.
- `--cores all n`
`all` is a convenient identifier that means all components.

`--crash-info n, -a`

Collect the latest *n* core directories (excluding the core files in those directories) for the following processes:

- `mta`
- `bmagent`
- `imrelay`
- `bmserver`
- `conduit`
- `jlu-controller`
- `dds`

The valid range for *n* is 1 through 9,999.

`--edm, -e`

Collect the exact data match (EDM) record sets.

`--find-other-cores, -d`

Discover any core file outside of `/data/scanner/jobs` and move them to `/data/scanner/jobs/other`.

If Symantec Messaging Gateway discovers and moves any core files, an email notification is sent to the administrators that are specified to receive alerts. If not, no email notification is sent.

You can use this option with the `delete cores` command to clean up core files on your product. Run this command first to move the core files that are not in the jobs directory to the jobs directory. Then use `delete cores` to delete the core files.

If `--find-other-cores` is the only data collection option specified, a URL is not required. No diagnostics package is generated.

`--force, -f`

Force diagnostics to run even if a diagnostics collection that is started from the user interface is still in progress. If a package creation is in progress, the existing diagnostics collection fails.

`--gcore, -g component`

Generate a core image of the specified component and download it. You can use this option to capture necessary data regarding a hung or spinning component, before restarting the component. This option does not stop or restart a process, but it may cause the process to pause briefly. The available components are:

- `bmagent`
- `bmserver`
- `conduit`
- `imrelay`
- `mta`
- `jlu-controller`

`--help, -h`

Display this message.

`--include-old-queues, -i`

Collect queue data from old postfix queues.

This command is only useful on configurations in which Symantec Messaging Gateway is migrated from version 7.7 or earlier. This command is not applicable for Symantec Messaging Gateway version 8 or higher.

`--ldap, -p`

Collect legacy ldapsync data.

This command is only useful on configurations in which Symantec Messaging Gateway is migrated from version 8 or earlier. This command is not applicable for Symantec Messaging Gateway version 9 or higher.

`--logs all, -l`

Collect all logs of all log files.

`--logs n, -l`

Collect log data that is limited to *n* lines per log file.

The valid range for *n* is 1 through 2,147,483,647.

`--monitor, -m`

Collect a snapshot output of the following `monitor` command: `monitor -c 6 --proc bmservice --proc mta system database disk mta p_all` and existing monitor logs under `/data/monitor`.

`--rules, -r`

Collect all rules that are present on the Scanner, except exact data match data.

`--tracking, -t`

Collect Message Audit Log files.

`--verbose, -v`

Show the command process in verbose mode.

ARGUMENTS

The syntax for the URL paths referenced by this command is as follows:

- `scp://user:'password'@host[:port]/path`
Copies the diagnostics package remotely through SCP.
- `ftp://user:'password'@host[:port]/path`
Copies the diagnostics package remotely through FTP.
If no user name and password are specified, an anonymous login is used.

Logon is attempted with the user name and password credentials that are provided on the command line. If special characters are included in the password, you must enclose the password in single quotes ('). If the special characters in a password include a single quote, you can use the double quote instead ("). If no credentials are specified, anonymous logon is used.

EXAMPLES

Create a diagnostics file and transfer it with the SCP protocol. The diagnostics file (in the format: `diagnostics.yy-yyy-dd-hh-mm.hostname.tar.gz`) is transferred to the SCP destination.

```
diagnostics scp://'support'@10.160.248.128/tmp/
```

Note: The month is expressed in the three-letter format, not two-digit format.

dns-control

`dns-control` - control the local DNS cache

SYNOPSIS

`dns-control` *command*

DESCRIPTION

The `dns-control` command manages local caching for the name server.

All `dns-control` command outputs end with either a completion message or a failure message. Examples are: "Command cmdname completed successfully" and "Command cmdname failed."

Some commands require the DNS cache to be running before they can be executed. In these cases, the only output is: "The DNS Cache is currently stopped." Start the cache with the `dns-control start` command before you run those commands.

ARGUMENTS

The command components are as follows:

`start`

Start the local caching name server.

`stop`

Stop the local caching name server.

`restart`

Restart the local caching name server.

`status`

Display the status of the local caching name server.

`flush`

Flush the cache.

`list`

List the locally configured name servers for the resolver.

`trace`

Increment the tracing (debug) level by +1.

`notrace`

Disable tracing (debug).

`reconfig`

Forces a reload of the name server configuration information.

`help`

Display this page.

grep

`grep` – search in files for text or a regular expression

DESCRIPTION

The `grep` command searches in the files that you specify for text or regular expressions.

Type `grep --help` on the command line for more information about the options available for `grep`. The information that is displayed may contain references to commands that are not available on Symantec Messaging Gateway.

This command is a standard Linux command that is limited in Symantec Messaging Gateway. Administrators can only use `grep`:

- On filenames obtainable through the `list` command.
- By piping the output of other commands to the `grep` command.

help

`help` – Display help for individual commands or display all available commands.

SYNOPSIS

```
help [ --list | command ]
```

DESCRIPTION

The `help` command displays a list of available commands on the product. If you specify a command name, the `help` command displays help for that command.

The help for commands is presented in Linux man page format. These help pages use the following Linux man page conventions. Do not type the brackets, parenthesis, or pipe symbol when you run a command.

Brackets []

The options and the arguments that are listed within square brackets are optional. The options and the arguments that are not listed within square brackets are required.

Parenthesis ()

The options and the arguments that are listed within parenthesis are required but are mutually exclusive. A pipe symbol separates the mutually exclusive options or arguments.

Pipe |

The pipe symbol indicates the options or arguments that are mutually exclusive. For example [*-e pattern* | *-f file*] means that you can specify *-e pattern* or *-f file*, but not both.

Colored, italic, or underlined text

Text that is italic, colored, or underlined indicates that you should substitute that text with specific text. When you type `help command`, the terminal or terminal software that you use to access the command line determines how this text appears. When you view help pages in a PDF or in the online help, this type of text is italic.

`--option`, `-o`

Some command options are available in long and short versions. The long version and short version produce the same behavior. Use whichever version is most convenient for you. In the OPTIONS section, these options are displayed with the long version first, followed by a comma, and then the short version. The long version is preceded with two dashes and the short version

is preceded with one dash. Some options have required parameters that you specify after the option, like a log level or IP address.

The help pages contain the following sections:

SYNOPSIS

A description of the options and arguments available for the command.

DESCRIPTION

General information about the command.

OPTIONS

Options that you can use to control the behavior of a command. Options always begin with one or two dashes, such as `-s` or `--status`. If an option is listed in square brackets in the synopsis, the options are optional. If not, the option is required.

Some options have arguments. For example, `--log level`. Square brackets indicate optional arguments.

Not all commands have options.

ARGUMENTS

Some commands require arguments. Arguments are names of files, host names, IP addresses, and so on that you specify to control the behavior of the command. Not all commands have arguments.

EXAMPLES

The EXAMPLES section provides sample command usage. Not all commands have examples.

SEE ALSO

The SEE ALSO section lists related commands. Not all commands have see also references.

Use the following commands to navigate through the help pages:

`f` or `SPACE`

Forward one screen

`b`

Backward one screen

`/pattern`

Search for a word or pattern

`<`

Go to the beginning of the document

>	Go to the end of the document
q	Exit from the document and display the command prompt
h	Display additional information about navigating the help pages

OPTIONS

<code>--list, -l</code>	Display a list of all the available commands.
-------------------------	---

ARGUMENTS

<i>command</i>	Display help for the specified command. If you do not specify a command, help for the <code>help</code> command is displayed (this page). Specify one of the following commands:
<code>agent-config</code>	Configures the agent that connects hosts to the Control Center
<code>cat</code>	Standard Linux command to view a file
<code>cc-config</code>	Configures the logging and network access to the Control Center
<code>clear</code>	A standard Linux command to clear the screen
<code>db-backup</code>	Back up the Control Center database
<code>db-restore</code>	Restores the Brightmail databases to an appliance from previously created backups on the appliance or from remote locations with FTP, SCP, and HTTP
<code>delete</code>	Clear logs, configuration information, and data
<code>diagnostics</code>	Generate diagnostics package

`dns-control`

Control the local DNS cache

`grep`

A standard Linux command to search in files for text or a regular expression

`help`

Display help for individual commands or display all available commands

`ifconfig`

A standard Linux command to configure network interfaces

`iostat`

A standard Linux command to display CPU and device load

`ldapsearch`

A standard Linux command to query an LDAP directory

`list`

Display the file names of all files that certain commands can act on

`mallog`

List, backup, or restore Message Audit Logs

`malquery`

Query Message Audit Logs

`monitor`

View and record information about Brightmail-specific processes

`more`

A standard Linux command to page through a text file

`mta-control`

Control the MTA processes and backup and restore mail queues

`netstat`

A standard Linux command to view network connections

`nslookup`

A standard Linux command to query DNS servers

`password`

Change your administrative password

`ping`

A standard Linux command to test for a response from a remote computer

`reboot`

Reboot the appliance

`route`

A standard Linux command to show and manipulate the IP routing table

`rpmdb`

Manage and repair the RPM database

`service`

A standard Linux command to start or stop services

`show`

Display system information

`shutdown`

Shut down the appliance without rebooting

`sshd-config`

Configure which addresses can SSH to the appliance

`tail`

A standard Linux command to view the end of a file

`telnet`

A standard Linux command to connect to a remote computer

`traceroute`

A standard Linux command to view the path that network packets take

`update`

Update the appliance software

HISTORY

In Symantec Brightmail Gateway version 9.0, some commands that existed in version 8.0 and previous versions were renamed, incorporated into other commands, or removed. The following commands were changed in version 9.0:

`agentconfig`

Replaced with `agent-config`.

`clear`

Replaced with `delete`. In version 9.0, the `clear` command clears the screen.

`crawler`

Part of `diagnostics`.

`date`

Replaced with `show --date`.

`deleter`

Replaced with `delete cores`.

`dn-normalize`

The functionality of the `dn-normalize` **command is not available in version 9.0.**

`eula`

Replaced with `show --eula`.

`http`

Replaced with `cc-config http`.

`install`

Replaced with `update install`.

`ls`

Replaced with `list`.

`mta-stats`

Replaced with `monitor mta`.

`passwd`

Replaced with `password`.

`pause-mode`

Replaced with `mta-control pause-mode`.

`rebuildrpmdb`

Replaced with `rpmdb --repair`.

`rm`

Replaced with `delete files`.

`set-control-center-port-443`

Replaced with `cc-config port-443`.

`sshdctl`

Replaced with `sshd-config`.

`sshdver`

Replaced with `sshd-config --version`.

`sys-info`

Replaced with `show --info`.

`system-stats`

Replaced with `monitor system`.

`tls-ca-cert-control`

The functionality of the `tls-ca-cert-control` command is not available in version 9.0.

ifconfig

`ifconfig` – a standard Linux command to configure network interfaces

DESCRIPTION

The `ifconfig` command displays the status and configuration of network interfaces and can make temporary changes to interface configurations.

Type `help ifconfig` on the command line for more information about the options available for `ifconfig`. The information that is displayed may contain references to commands that are not available on Symantec Messaging Gateway.

This command is a standard Linux command that has not been modified.

iostat

`iostat` – a standard Linux command to display CPU and device load

DESCRIPTION

The `iostat` command monitors system input/output device loading by observing the time devices are active in relation to their average transfer rates.

Type `help iostat` on the command line for more information about the options available for `iostat`. The information that is displayed may contain references to commands that are not available on Symantec Messaging Gateway.

This command is a standard Linux command that has not been modified.

ldapsearch

`ldapsearch` – a standard Linux command to query an LDAP directory

DESCRIPTION

The `ldapsearch` command searches in the LDAP source that you specify and displays matching records.

Type `help ldapsearch` on the command line for more information about the options available for `ldapsearch`. The information that is displayed may contain references to commands that are not available on Symantec Messaging Gateway.

This command is a standard Linux command that has not been modified.

list

`list` – display the file names of all files that certain commands can act on

SYNOPSIS

```
list [--all] [--cores] [--diagnostics] [--logs] [--monitor] [--temp]
[--top]
list --help
```

DESCRIPTION

The `list` command displays the file names of all of the files that can be acted upon by certain commands. The following commands can act upon the files that are listed with `list`:

`cat`

Display the contents of one or more files.

`delete`

Delete one or more files.

`more`

Display the contents of one or more files and pause at the end of each screen.

`tail`

Show the last 50 lines of the named log file.

OPTIONS

If `list` does not list any files when you specify an option, there are no files in that category.

`--all, -a`

List all files.

`--cores, -c`

List all core files.

`--diagnostics, -d`

List all diagnostic packages.

`--help, -h`

Display this message.

`--logs, -l`

List all log files.

`--monitor, -m`

List all monitor files.

`--temp, -p`

List all temporary files.

`--top, -t`

List the largest files that the administrator can delete and their sizes.

EXAMPLES

Example 1

List all the files that can be viewed with `cat` (except core files and diagnostic files) or deleted with `delete`.

```
list --all
```

Example 2

List the largest files that you can delete. You can use the `delete` command to delete large files if you do not need them.

```
list --top
```

SEE ALSO

See [cat](#) on page 16.

See [delete](#) on page 27.

See [more](#) on page 66.

mallog

mallog – list, backup, or restore Message Audit Logs

SYNOPSIS

```
mallog [ --list ]  
mallog [ --backup | --restore ] url
```

DESCRIPTION

The `mallog` command backs up and restores Message Audit Log data that resides on the Scanner. The `mallog` command also lists the Message Audit Log files on the Scanner. To view message activity in the Message Audit Logs, use the Control Center or the `malquery` command.

Available log files include the following:

- /data/logs/scanner/audit_bmengine_log*
- /data/logs/scanner/audit_mte_log*
- /data/logs/scanner/audit_mta_log*

Note: When you run `mallog --backup` or `mallog --restore`, email processing stops while these commands run. No inbound email or outbound email is delivered during this time. If your organization's email availability policies are strict, it may be appropriate to only run these commands during off hours.

OPTIONS

`--backup url`

Create a backup of all of the message tracking logs that are in tar.gz format, and upload the resulting file to the specified URL.

Note: This option suspends mail processing while the command is executed.

`--list`

List individual message tracking logs on the file system and their timestamps and sizes.

`--restore url`

Restore message tracking logs from the specified URL. Existing logs are overwritten.

Note: This option suspends mail processing while the command is executed.

URLs may have a scheme of either FTP, SCP, or, HTTP (for restore only).

If you specify a path that ends with a forward slash, the diagnostics file is written to the path that you specify with the default file name. If you specify a path that does not end with a forward slash, the backup file is written with the file name specified in the path. The `--restore` option requires a full path name which includes a file name. The entire URL should be taken in double quotes. If any part of the URL contains special characters, such as full or double quotes, escape the special characters with a backslash. When the password is part of the URL, it should be written in quotes if it has any special shell characters in it.

url

Transmit the package to the *url* location by SCP or FTP.

The entire URL should be taken in double quotes. If any part of the URL contains special characters, such as full or double quotes, escape the special characters with a backslash. When the password is part of the URL, it should be written in quotes if it has any special shell characters in it.

SEE ALSO

See [malquery](#) on page 55.

malquery

malquery - query Message Audit Logs

SYNOPSIS

```
malquery (-l start,end | -g start,end)
(-u uid [-u uid ...] | -e event[,arg_num]<=|*>string [-e ...] | -q
event[,arg_num]<=|*>quoted-printable-string [-q ...])
[-m max_results] [-I index_max] [-o output_file] [-v]
```

DESCRIPTION

You can track messages in the Control Center by querying the Message Audit Logs. Alternatively, you can use the `malquery` command-line command to track messages. Use `malquery` instead of the Control Center for complex queries or queries where you expect voluminous data. The `malquery` command only returns data for the Scanner that you are logged into.

Enabling Message Audit Logging results in approximately 800 bytes of audit logs per message. Message Audit Logging can cause performance and storage problems if your site receives more than 1,000,000 messages per day.

Audit logs older than the current day are rolled over to a filename appended with the local date in the form `yyyymmdd`. Audit logs older than the default retention period of 30 days are deleted.

The output from `malquery` is in `.xsd` format, for example:

```
<malResults count="message result count">
  <message UID="uid">
    <events>
      <event time="utc" name="event id">parameters</event>
      <event time="utc" name="event id">parameters</event>
      <event time="utc" name="event id">parameters</event>
      <event time="utc" name="event id">parameters</event>
    </events>
  </message>
</malResults>
```

OPTIONS

-e ...

Find email messages that contain the events that match the specified criterion.

Examples:

`-e RCPTS=dale@company.com`

RCPTS is recipient. In this example, the recipient is dale@company.com.

`-e SUBJECT*"my flowers"`

SUBJECT is the subject of the email message. In this example, the subject contains the words 'my flowers'.

`-g start,end`

Find messages by the GMT date range to search in UNIX time (the number of time units that have elapsed since the epoch time 1/1/1970). For example, July 4, 2008, 11:59 P.M. = 1215212340.

Separate the start date and end date by a comma with no space.

`-I index_max_n`

Use the index (.idx file) if the number of matching results is less than or equal to *index_max_n*. Otherwise, the index is ignored. This option searches a flat file, which saves time when you want to look up large numbers of events.

The default for *index_max_n* is 1000.

`-l start,end`

Find messages based on the specified date range. The date format is YYYYMMDDhhmm. For the hours and minutes, use a 24-hour clock. For example:

July 4, 2008, 11:59 P.M. = 200807042359.

Separate the start date and end date by a comma with no space.

`-m max_results`

Return the *max_results* number of messages. The default is 1000.

`-o file`

Output data that matches results to *file*.

`-q ...`

Find email messages that contain the events that match the specified criterion in quoted-printable encoding. For example:

`-q SUBJECT*"red =3D rose" -- subject contains 'red = rose'`

`-u audit_id`

Find the email message with the specified audit ID.

`-v`

Show the command process in verbose mode.

EXAMPLES

Example 1

Search for an email based on the following criteria:

- Start date is between July 4, 2008, 2:00 P.M. and date of July 4, 2008, 11:59 P.M. in GMT time
- Recipient is “dale@company.com”
- Subject contains the words “check this out”
- Maximum output is 500 results
- Write results to file /tmp/results.xml

```
malquery -g 1215140340,1215212340 -e RCPTS=dale@company.com -e  
SUBJECT*"check this out" -m 500 -o /tmp/results.xml
```

Example 2

Search for an email based on the following criteria:

- Start date is between July 4, 2009, 11:00 P.M. and date of July 4, 2009, 11:59 P.M.
- Recipient is “dale@company.com”
- The audit ID of *uid number*
- Maximum output is 500 results
- Write results to file /tmp/results.xml

```
malquery -l 200907042300,200907042359 -e RCPTS=dale@company.com -uid  
uid number -m 500 -o /tmp/results.xml
```

Example 3

Search for an email based on the following criteria:

- Start date is between July 4, 2009, 11:00 P.M. and date of July 4, 2009, 11:59 P.M.
- Recipient is “dale@company.com”
- Subject contains the quoted-printable encoding words that return the email messages that match the word “red” in the subject. For example: “red roses”.
- Maximum output is 500 results
- Write results to file /tmp/results.xml

```
malquery -l 200907040000,200907090000 -e RCPTS=dale@company.com -q  
SUBJECT*"red " -m 500 -o /tmp/results.xml
```

Example 4

Search for an email based on the following criteria:

- Start date between July 4, 2009, 11:00 P.M. and date of July 4, 2009, 11:59 P.M.
- Recipient is “dale@company.com”
- Subject contains the words "check this out"
- Number of matching results for this command is the default index_max of 1000
- Write results to file /tmp/results.xml

```
malquery -l 200907040000,200907090000 -e RCPTS=dale@company.com -e  
SUBJECT*"check this out" -I -o /tmp/results.xml
```

SEE ALSO

See [mallog](#) on page 53.

monitor

`monitor` – view and record information about Brightmail-specific processes

SYNOPSIS

```
monitor options [--proc name] [identifier ...]  
monitor list  
monitor stop ( pid | all )
```

DESCRIPTION

The `monitor` command lets you view and record detailed information about the Brightmail system and its processes.

OPTIONS

`--count, -c num`

Produce *num* samples.

The default is 1. The upper limit is $2^{31}-1$ (roughly, 2.1 billion).

`--help, -h`

Display this message.

`--interval, -i num`

Take a sample at the *num* interval (measured in seconds).

The default is 10 seconds. For any long-running monitor jobs that are written to disk, you should increase this interval (to 60 or more). If the disk space fills up, the `monitor` process stops. Increase the interval time to avoid this issue.

`--output, -o file`

Save the output to a file instead of printing it to the console. The file is saved as `/data/monitor/file`.

When you use this option, `monitor` runs in the background and returns the process ID (PID) of the monitor process. Use `cat`, `more`, or `tail` to view the file. The file name can contain ASCII characters.

`--proc, -p name`

Collect data for one of the following Brightmail processes and its children. The valid process names and the programs that they represent are as follows:

`afasnmppd`

The `afasnmppd` process provides SNMP information for some Dell PowerEdge Expandable RAID Controllers.

The `afasnmppd` process is only applicable on the following systems:

- Dell System PowerEdge 750 (SMS 8240) appliance
- Dell System PowerEdge 850 (one of many SMS 8340) appliance

`bmagent`

The Brightmail Agent facilitates communicating configuration information between the Control Center and each Scanner.

`bmserver`

The `bmserver` process filters email messages.

`conduit`

The Conduit retrieves updated email filters and manages statistics.

`controlcenter`

The Control Center provides centralized Web administration, collects statistics, and hosts quarantines.

`im`

The IM process filters instant messaging.

`liveupdate`

LiveUpdate downloads virus definitions from Symantec Security Response to the Scanner.

`lsisnmppd`

The `lsisnmppd` process provides SNMP information for some Dell PowerEdge Expandable RAID Controllers.

The `lsisnmppd` process is only applicable on the following systems:

- Dell System PowerEdge 1950 (SMS 8360) appliance
- Dell System PowerEdge 2950 (SMS 8380) appliance
- Dell System PowerEdge R610 (SMS 8360) appliance
- Dell System PowerEdge R710 (SMS 8380) appliance
- Dell System PowerEdge 860 (SMS 8340) appliance
- Dell System PowerEdge R200 (SMS 8340) appliance
- Dell System PowerEdge R210 (SMS 8340) appliance

monitor

The **monitor** process displays or saves information about Symantec Messaging Gateway processes.

mta

The mail transfer agent routes inbound and outbound messages to the Brightmail Engine for processing and delivers filtered messages.

mysql

The MySQL database on the Control Center stores settings and message information.

percsnmpd

The **percsnmpd** process provides SNMP information for some Dell PowerEdge Expandable RAID Controllers.

The **percsnmpd** process is only applicable on the following system:

- Dell System PowerEdge 1850 (SMS 8260) appliance

snmpd

The **snmpd** process waits for requests from SNMP management software.

stunnel

The **stunnel** process provides secure encrypted connections.

--quiet, -q

Suppress any warnings from the monitor program.

--tab, -t

Produce data in a tabular format. Use the **--tab** option with the **--output** option to create output to import into a spreadsheet. The **--tab** does not format text correctly for the screen. For example, on the screen the column headings are not aligned with the column data.

When you format data for tabular output **--tab**, the column headings for each identifier are prefaced with the process name. For example,

`controlcenter_p_%user.`

ARGUMENTS

list

Produce a list of all monitor processes, their PIDs, and the options that were used at runtime. The **monitor list** command always shows the **monitor list** command as one of the monitor processes that is running. This behavior is normal.

```
stop ( pid | all )
```

Stop the specified monitor processes. Type a PID to stop a single process.
Type the word `all` to stop all monitor processes.

identifiers

The information that is displayed or saved depends on the identifiers that you specify. If you do not specify one or more identifiers, then the default of `system` is used. Some identifiers represent multiple identifiers and are provided for convenience. Five groups of identifiers are available: `system`, `database`, `disk`, `MTA`, and `process`.

System identifiers are as follows:

- `%user` - Percent of the available CPU time that is spent in user mode.
- `%nice` - Percent of the available CPU time that is spent running as nice.
- `%sys` - Percent of the available CPU time that is spent in system mode.
- `%wait` - Percent of the available CPU time that is spent in IO wait.
- `%idle` - Percent of the available CPU time that is spent idling.
- `memt` - Total memory (k)
- `memu` - Memory in use (k).
- `pageout` - The number of memory pages that are swapped out to disk.
- `system` - A convenience identifier that includes the following system identifiers: `%user %sys %wait memt memu memf`.

Database Identifiers - These identifiers denote the size of the Control Center database, the size of its various quarantines, and how many messages they contain. The identifiers are as follows:

- `db_size` - The total size of the Control Center database in kilobytes.
- `db_qsize` - The size of the Spam Quarantine directory kilobytes.
- `db_qqty` - The number of messages in the Spam Quarantine.
- `db_vsize` - The size of the Suspect Virus Quarantine directory, in kilobytes.
- `dv_vqty` - The number of messages in the Suspect Virus Quarantine.
- `db_csize` - The size of the content incident directories.
- `db_cqty` - The number of messages in the content incident quarantine.
- `database` - A convenience identifier that includes all the database identifiers.

Disk identifiers - The disk identifiers provide information on disk utilization on the partitions that the administrator controls. The identifiers are as follows:

- `data_used` - The percentage of `/data` that is being used.
- `data_free` - The amount of free space in `/data`, in kilobytes.
- `opt_used` - The percentage of `/opt` that is being used.
- `opt_free` - The amount of free space in `/opt`, in kilobytes.
- `other_used` - The percentage of `/opt` that is being used (for example, 20%).
- `other_free` - The amount of space available on `/opt` in kilobytes.
- `disk` - A convenience identifier that includes all the above disk data.

MTA identifiers - These identifiers report MTA statistics. The identifiers are as follows:

- `i_conn` - Number of inbound connections.
- `i_qmsgs` - Number of queued inbound messages.
- `i_dmsgs` - Number of deferred inbound messages.
- `i_qsize` - Size of the inbound queue (MBs).
- `i_drte` - Inbound listener data rate (kbps).
- `i_mrate` - Inbound listener message rate.
- `mta_in` - All of the inbound statistics (the identifiers that begin with `i_`).
- `o_conn` - Number of outbound connections.
- `o_qmsgs` - Number of queued outbound messages.
- `o_dmsgs` - Number of deferred outbound messages.
- `o_qsize` - Size of the outbound queue (MBs).
- `o_drte` - Outbound listener data rate (kbps).
- `o_mrate` - Outbound listener message rate.
- `mta_out` - All of the outbound statistics (the identifiers that begin with `o_`).
- `d_conn` - Number of delivery connections.
- `d_qmsgs` - Number of queued delivery messages.
- `d_dmsgs` - Number of deferred delivery messages.
- `d_qsize` - Size of the delivery queue (MBs).

- `d_drate` - Delivery listener data rate (kbps).
- `d_mrate` - Delivery listener message rate.
- `mta_del` - All of the delivery statistics (the identifiers that begin with `d_`).
- `mta` - A convenience identifier that includes all of the MTA identifiers.

The information that is collected depends on the identifiers that are provided. If none are provided, then the default of “system” is used. Some identifiers represent multiple identifiers and are provided for convenience. This command does not give any indication about the average load or amount of work that is done between one sample and the next. Each sample is a snapshot of the MTA status at that point in time.

Process identifiers - The `--proc` option lets you monitor statistics for groups of Brightmail processes. If the `--proc` flag is used without any `p_*` identifiers, the following default value is used: `p_%user p_%sys p_memv p_memr p_mems`. Identifiers for use with `--proc` include:

- `p_%user` - Percent of the available CPU time that is spent in user mode.
- `p_%sys` - Percent of the available CPU time that is spent in system mode.
- `p_memv` - Virtual memory that the processes use (k).
- `p_memr` - Resident memory in use by the processes (k).
- `p_mems` - Highest amount of the shared memory that any of the processes use (k).
- `p_all` - All of the proc identifiers.

EXAMPLES

The following examples describe some ways that you can use the `monitor` command. These examples include a mix of the long and short forms of some of the option names, such as `-o` and `--output`.

Example 1

Check one time the percent of available CPU time and memory that the conduit service consumes. Save the result to file `/data/monitor/conduit_mon`.

```
monitor --proc conduit --output conduit_mon
```

Example 2

Collect the average load of the MTA service on the system every 3 seconds 1000 times. Display the average load on the system from the MTA service in a tabbed format and written out to file `/data/monitor/mta_mon`.


```
monitor --proc mta --interval 3 --count 1000 --tab --output mta_mon
```

Example 3

Collect the average load of the `afasnmppd` service on the system every 3 seconds 1000 times. Display the average load on the system from the MTA process in a tabbed format and saved to file `/data/monitor/snmp_mon`. Normally, no output appears on the screen because of the `-q` option.

```
monitor --proc afasnmppd --interval 3 --count 1000 --tab -q -o snmp_mon
```

Example 4

Check one time the percent of available CPU time and the memory that the LiveUpdate service uses. Save the result to file `/data/monitor/liveupdate_mon`.

```
monitor --proc liveupdate --output liveupdate_mon
```

Example 5

Check one time the percent of available CPU time and the memory that the monitor service consumes. Save the result to file `/data/monitor/monitor_mon` in tabbed format.

```
monitor --proc monitor --output monitor_mon --tab
```

Example 6

Check the percent of available CPU time and the memory the stunnel service consumes. Save the result to file `/data/monitor/stunnel_mon` in tabbed format. Normally, no output appears on the screen because of the `--quiet` option.

```
monitor --proc stunnel --output stunnel_mon --tab --quiet
```

SEE ALSO

See [cat](#) on page 16.

See [delete](#) on page 27.

See [list](#) on page 51.

See [more](#) on page 66.

See [tail](#) on page 87.

more

`more` – a standard Linux command to page through a text file

DESCRIPTION

The `more` command displays the contents of plain text files one screen at a time. Press **Space** to view the next screen. Use the `list` command to list the files that `more` can display.

You can run the output of another command to `more` to view the output one screen at a time. After the command that you are running, type the pipe symbol and then `more`. See the example below.

Type `help more` on the command line for more information about the options available for `more`. The information that is displayed may contain references to commands that are not available on Symantec Messaging Gateway.

The `more` command is a standard Linux command that has been modified to only display the files that the `list` command shows.

EXAMPLES

Example 1

Display `BrightmailLog.log` one screen at a time.

```
more /data/logs/bcc/BrightmailLog.log
```

Example 2

Examine the output of `list --top` one screen at a time.

```
list --top | more
```

SEE ALSO

See [list](#) on page 51.

mta-control

`mta-control` – control the MTA processes and backup and restore mail queues

SYNOPSIS

```
mta-control queue command
mta-control pause-mode mode
```

DESCRIPTION

The `mta-control` command lets you query MTA queues, and control specific elements within MTA message processing. For example, you can flush message queues.

Note: Do not use the ~ (tilde) character when you specify output file names, paths, passwords, email addresses, and user names (for exporting). Specify the full path name.

ARGUMENTS

Specify one of the following MTA queues:

- inbound
- outbound
- delivery
- all

The following components are available:

- start – Start the queue.
- stop – Stop the queue.
- status – Display the current status. The status can be: running, not running, enabled, or disabled.
- restart – Restart the queue.
- flush – Reattempt delivery for all queued messages.
- delete-msgs-by-sender *regex* – Delete from the queue all messages with Envelope Sender that matches the given Perl regular expression (case insensitive).

- `delete-msgs-by-rcpt regex` – Delete from the queue all messages with an Envelope Recipient that matches the given Perl regular expression (case insensitive).

Note: This deletes the entire message, not just the recipient.

- `delete-msg-by-id queue-ID` – Delete the message with the given queue-ID from the queue.
- `delete-all-msgs` – Delete all messages from the queue.
- `active-routes` – Print all active routes and the number of messages for each route.
- `num-messages-in-route route` – Print the number of messages for the given route.
- `list-msgs route` – Print the messages for the given route.
- `list-msg-details msgid` – Given a message ID, print details about that message.
- `route-info route` – Display DNS lookup information, destination, and number of messages for a route.
- `reroute src-routedst-route` – Reroute messages from *src-route* to *dst-route*.
- `delete-msgs-by-sender perl regex` – Delete from the queue all messages with an envelope sender that matches the given Perl regular expression (case insensitive).
- `delete-msgs-by-rcpt perl regex` – Delete from the queue all messages with an envelope recipient that matches the given Perl regular expression. Note that this deletes the entire message, not just the recipient (case insensitive).
- `delete-msg-by-id queue-ID` – Delete the message with the given queue-ID from the queue. Note that the ID is only unique per queue.
- `delete-all-msgs` – Delete all messages from the queue.
- `import-queues url` – Import an entire mail queue from backup. Specify `all` for the queue. Ensure that the MTA is running before importing a mail queue. To start the MTA, run `mta-control all start`. Specify the URL as described for the `export-msg-by-id` component.
- `export-queues url` – Back up the mail queue to a URL. Specify `all` for the queue. Ensure that the MTA is stopped before exporting the mail queue. To stop the MTA, run `mta-control all stop`. Specify the URL as described for the `export-msg-by-id` component.

- **export-msg-by-id** *queue-ID* [*url*] – Export the message with the given queue-ID from the queue and save it to the specified URL. If you do not specify a URL, the message data is displayed on the screen. If you do not specify the FTP password, `mta-control` prompts you for the password. If you specify a path that ends with '/', Symantec Messaging Gateway stores the file in that location using a default file name. Otherwise, Symantec Messaging Gateway stores the file with the file name that you specified in the path. The URL syntax is as follows:

`scp://'user'@host/path` (user is prompted for password)

`ftp://'user':password@host[:port]/path`

`ftp://'user'@host[:port]/path`

Put a double-quote character before and after the URL. If any part of the URL contains special characters, such as full or double quotes, put a backslash before each special character.

- **query-queue** – Query the message queue.
The following optional parameters are accepted:

- `sender_match=perl regexp`

- `rcpt_match=perl regexp`

- `deferred` - selects the messages that are deferred

- `include_subject`

- `start=N`

- `limit=N`

- `format=neat/xml`

The parameters `sender_match`, `rcpt_match` and `deferred` are logically ANDed together if present. The intermediate result set after applying these matches is sorted by date, and then the start and limit are applied: `\$start` messages are skipped and then `\$limit` messages are returned. The default is to show all messages in 'neat' format, which is meant to be human readable.

- **bad-msg-list** – List the times and IDs of messages in the bad message queue. The queue is either inbound or outbound.
- **bad-msg-export** *queue-ID* [*url*] – Export or display the message. See `export-msg-by-id` for URL format.
To display the message on the screen, type `mta-control queue bad-msg-export queue-ID`.
Specify the URL as described for the `export-msg-by-id` component.
- **bad-msg-delete** *queue-ID* – Delete the message.

- **bad-msg-bypass *queue-ID*** – Submit the message for delivery to the original recipients and bypass scanning.
- **bad-msg-forward *queue-IDaddress*** – Submit a copy of the message for delivery to the given address and bypass scanning. The original bad message remains in the bad message queue.
- **bad-msg-retry *queue-ID*** – Retry scanning the message as if it were new.

The six pause modes affect email scanning (*scan*), acceptance (*accept*), and delivery (*delivery*). Each pause mode sets scanning, acceptance, and delivery to a particular state as described below, regardless of the previous state of *scan*, *accept*, and *delivery*. Pause modes are as follows:

- **status** – Display the current pause mode status. If you type `mta-control pause-mode`, `mta-control` displays the pause mode status.
- **pause-accept** – Set *scan* to running and set *accept* to paused. The *delivery* state is not affected by *pause-accept*.
- **pause-deliver** – Set *delivery* to paused. The *accept* and *scan* states are not affected by *pause-deliver*. This is equivalent to `mta-control delivery stop`.
- **pause-scan** – Set *scan* to paused and set *accept* to running. The *delivery* state is not affected by *pause-scan*.
- **resume-accept** – Set *scan* to running and set *accept* to running. The *delivery* state is not affected by *resume-accept*.
- **resume-deliver** – Set *delivery* to running. The *accept* and *scan* states are not affected by *resume-deliver*. This is equivalent to `mta-control delivery start`.
- **resume-scan** – Set *scan* to running and set *accept* to running. The *delivery* state is not affected by *resume-scan*.

EXAMPLES

Example 1

Show the status of the MTA (inbound, outbound, and delivery queues and whether they are running or not).

```
mta-control pause-mode status
```

Example 2

Do not accept any new mail on the appliance but scan mail in the queue. This command does not affect the delivery of email.

```
mta-control pause-mode pause-accept
```

Example 3

Accept email on the appliance, but do not scan it. This command does not affect the delivery of email.

```
mta-control pause-mode pause-scan
```

Example 4

Do not deliver email on the appliance.

```
mta-control pause-mode pause-deliver
```

Example 5

Accept and scan email on the appliance. This command does not affect the delivery of email.

```
mta-control pause-mode resume-accept
```

Example 6

Accept and scan email on the appliance. This command does not affect the delivery of email.

```
mta-control pause-mode resume-scan
```

Example 7

Deliver email on the appliance.

```
mta-control pause-mode resume-deliver
```

Example 8

Display the queue-id of messages in delivery queue.

```
mta-control delivery query-queue
```

Example 9

View a raw message in the delivery queue with a message queue-id.

```
mta-control delivery export-msg-by-id 00/00-25597-EFD46794
```

Example 10

Export a specific message from the delivery queue with a message queue-id. The message queue-id is 00/00-25597-EFD46794. Export it to the 192.168.159.99 SCP server in the /tmp directory with the support account. `mta-control` queries for the password.

```
mta-control delivery export-msg-by-id 00/00-25597-EFD46794  
"scp://support\@192.168.159.99/tmp/"
```

Example 11

Export all message queues. Export the message queue file to the 192.168.159.99 FTP server in the /tmp directory with the sysadmin account. Since a password is not specified, `mta-control` queries for the password.

```
mta-control all export-queues "ftp://sysadmin\@192.168.159.99/tmp/"
```

Example 12

```
mta-control all query-queue
```

Show all messages currently in the inbound queue, the outbound queue, and the delivery queue.

netstat

`netstat` – a standard Linux command to view network connections

DESCRIPTION

The `netstat` command prints network connections, routing tables, interface statistics, masquerade connections, and multicast memberships.

Type `help netstat` on the command line for more information about the options available for `netstat`. The information that is displayed may contain references to commands that are not available on Symantec Messaging Gateway.

This command is a standard Linux command that has not been modified.

EXAMPLES

Example 1

Display network connections.

```
netstat -an
```

Example 2

Display routing table.

```
netstat -r
```

nslookup

`nslookup` – a standard Linux command to query DNS servers

DESCRIPTION

The `nslookup` command performs a DNS lookup of the given hostname or IP address.

Type `help nslookup` on the command line for more information about the options available for `nslookup`. The information that is displayed may contain references to commands that are not available on Symantec Messaging Gateway.

This command is part of the standard Linux command set. It has been modified for use by Symantec Messaging Gateway, but this modification does not affect its functionality.

EXAMPLES

Look up MX records for a domain (yahoo.com, for example):

```
nslookup -querytype=mx yahoo.com
```

password

`password` – change your administrative password

SYNOPSIS

`password [--help] [--reset]`

DESCRIPTION

The `password` command changes the password that you use to logon to the command line. You are prompted to type your old password, and to type your new password twice.

Note: If you are using the Control Center appliance when you change the password, the admin password for login to the Control Center is also changed.

OPTIONS

`--help, -h`

Display this message.

`--reset, -r`

Set the administrative password to the factory default.

ping

`ping` – a standard Linux command to test for a response from a remote computer

DESCRIPTION

The `ping` command tests, through data packet, the transfer of that data between the appliance and the hostname or IP address that you specify.

Type `help ping` on the command line for more information about the options available for `ping`. The information that is displayed may contain references to commands that are not available on Symantec Messaging Gateway.

This command is a standard Linux command that has not been modified.

reboot

`reboot` – reboot the appliance

SYNOPSIS

`reboot [--force]`

DESCRIPTION

The `reboot` command stops all services and then restarts the appliance.

Note: When prompted, you must type **yes** to complete shutdown. Typing **y** results in an error message.

Note: If you reboot the appliance while you run software update on Symantec Messaging Gateway, you can corrupt the appliance software.

OPTIONS

`--force, -f`

Reboot the appliance, even if software update is running (not recommended). The appliance can become corrupted and require reinstallation. Contact Symantec Technical Support for information about reinstalling the appliance software.

`--help, -h`

Display this message.

SEE ALSO

See [shutdown](#) on page 84.

route

`route` – a standard Linux command to show and manipulate the IP routing table

DESCRIPTION

The `route` command lets you view routing tables or add entries to a routing table temporarily. Its primary use is for viewing the routing tables.

Type `help route` on the command line for more information about the options available for `route`. The information that is displayed may contain references to commands that are not available on Symantec Messaging Gateway.

This command is a standard Linux command that has not been modified.

rpmdb

rpmdb – manage and repair the RPM database

SYNOPSIS

```
rpmdb [--verify] [--repair]
```

DESCRIPTION

The `rpmdb` command lets you verify the current RPM database and rebuild it. This command can be useful in the event the database is corrupted and you want to repair it. Software updates for Symantec Messaging Gateway are stored as RPM packages.

OPTIONS

`--repair, -r`

Rebuild the RPM database.

`--verify, -v`

Verify the current RPM database.

service

`service` – a standard Linux command to start or stop services

SYNOPSIS

```
service name command  
service name help
```

DESCRIPTION

Start, stop, and check the status of Symantec Messaging Gateway services with the `service` command. Services are programs that run continuously to perform specific tasks. During normal operation, you do not have to stop or start services. You may need to stop or start services to diagnose or resolve a problem with Symantec Messaging Gateway.

The `service` command is a standard Linux command that has been modified to work with services available on Symantec Messaging Gateway.

ARGUMENTS

Specify a service *name* and *command* when you run `service`.

name

Specify one of the following service names:

`afasnmppd`

The `afasnmppd` service provides SNMP information for some Dell PowerEdge Expandable RAID Controllers.

`agent`

The Brightmail Agent facilitates communicating configuration information between the Control Center and each Scanner.

`connector`

The Conduit and LiveUpdate services download spam and virus definitions.

`controlcenter`

The Control Center provides centralized Web administration, collects statistics, and hosts quarantines.

`dds`

Directory data service interfaces with LDAP to provide authentication, email address validation, message routing, and policy groups.

If you restart the `dds` service, the `bmclient_log` and `bmserver_log` log files may contain many `Could not connect: Connection refused` errors. These errors are normal.

`imrelayd`

The IM service filters instant messaging.

`lsisnmpd`

The `lsisnmpd` service provides SNMP information for some Dell PowerEdge Expandable RAID Controllers.

`mta`

The mail transfer agent processes, routes, and delivers email messages in cooperation with the Brightmail Engine.

`mysql`

The MySQL database on the Control Center stores settings and message information.

`osconfig`

The `osconfig` service manages network interfaces and related services.

`percsnmpd`

The `percsnmpd` service provides SNMP information for some Dell PowerEdge Expandable RAID Controllers.

`smsswapfile`

The `smsswapfile` service manages secondary swap file space.

`snmpd`

The `snmpd` service waits for requests from SNMP management software.

`stunnel`

The `stunnel` service provides secure encrypted connections.

`command`

The following commands are available. Some commands do not apply to certain commands. Type `service name help` to display the commands that apply to a service.

`condrestart`

Restart the service only if it is currently running. This command is available only for the `controlcenter`, `snmpd`, `mta`, and `stunnel` services.

`delete`

Delete the swap file on the appliance. This command is available only for the `smsswapfile` service.

`help`

Display the commands available for the service that you specify.

`reload`

This command is available only for the `mysql` and `stunnel` services.

`restart`

Stop the service and then start the service.

`status`

Display the status of a service.

`start`

Start the service.

`stop`

Stop the service.

EXAMPLES

Example 1

Display the commands that are available for the `mta` service.

```
service mta help
```

Example 2

Display the status of the `mta` service.

```
service mta status
```

Example 3

Stop the `mta` service.

```
service mta stop
```

Example 4

Stop the Conduit, LiveUpdate, and `jlu-controller`.

```
service connector stop
```

show

`show` – display system information

SYNOPSIS

```
show [--date] [--eula] [--info] [--version]  
show --help
```

DESCRIPTION

The `show` command displays the following information:

- Current date and time
- End User License Agreement
- System information
- Product version number

OPTIONS

`--date, -d`

Show the current date and time.

`--eula, -e`

Show the End User License Agreement.

`--help, -h`

Display this message.

`--info, -i`

Show the system hardware information.

`--version, -v`

Show the product version number and installation date.

shutdown

`shutdown` – shut down the appliance without rebooting

SYNOPSIS

`shutdown [--help | --force]`

DESCRIPTION

The `shutdown` command turns off the appliance immediately. The appliance is not restarted. Shutdown occurs immediately and email messages remain in the queues. To start an appliance after you run the `shutdown` command, you must press the appliance power button, unless you have configured remote access to the appliance hardware.

Note: When prompted, you must type **yes** to complete shutdown. Typing **y** results in an error message.

Note: If you shut down the appliance during the software update process, you can corrupt the appliance software.

OPTIONS

`--help, -h`

Display this message.

`--force, -f`

Shut down the appliance, even if software update is running (not recommended). The appliance can become corrupted and require reinstallation. Contact Symantec Technical Support for information about reinstalling the appliance software.

SEE ALSO

See [reboot](#) on page 77.

sshhd-config

sshhd-config - configure which addresses can SSH to the appliance

SYNOPSIS

```
sshhd-config (--list | --help)
sshhd-config --add (allow|deny) address
sshhd-config --delete (allow|deny) rule#
sshhd-config --version [1|2]
sshhd-config --cbc [on|off]
```

DESCRIPTION

The `sshhd-config` command lets you specify which addresses can access the appliance through SSH.

OPTIONS

`--add, -a`
Add a new rule.

`--cbc, -c`
Turn on or off support for CBC ciphers, also known as block ciphers. If set to `off`, the only cipher available for use is RC4, also known as arcfour.

`--delete, -d`
Delete an active rule.

`--help, -h`
Display this message.

`--list, -l`
Display the active rules and the current protocol number.

`--version, -v`
Set the version number of the protocol to use (1 or 2).

ARGUMENTS

`allow/deny`
When an SSH client connects, the client address is compared to the allow list and deny list in the following order:

- If the client address matches any allow rules, then the connection is allowed.
- If the client address matches any deny rules, then the connection is rejected.

`rule`

Each rule is a list of one or more addresses and wildcards that are separated by commas, as follows:

- `some.hostname.com`
Matches a specific host
- `.hostname.com`
Matches `some.hostname.com` and `other.hostname.com`
- `1.2.3.4`
Matches a specific IP address
- `1.2.`
Matches any IP address starting with 1.2
- `1.2.3.0/255.255.255.0`
Matches any IP address within the 1.2.3.* subnet
The EXCEPT keyword can be used to exclude a subset of addresses. For example, `hostname.com EXCEPT forbidden.hostname.com`.

You can specify one of the following keywords instead of a host name or IP address for the address parameter. Use the KNOWN and UNKNOWN keywords with care since they depend on DNS service.

- `ALL`
Matches any address
- `LOCAL`
Matches any host whose name does not contain a dot character
- `KNOWN`
Matches any host whose name and address are known
- `UNKOWN`
Matches any host whose name or address are unknown

tail

`tail` – a standard Linux command to view the end of a file

SYNOPSIS

```
tail [-f | --help ] log_name
```

DESCRIPTION

The `tail` command is part of the standard Linux command set which shows the last 50 lines of the named log file.

However, this command is modified in the following ways:

- Only the `-f` and `--help` options that are described here are available.
- If a character in a log file is not printable or is not ASCII, the sequence `\xAB` is displayed instead of that character. AB is the hexadecimal value of the character. For example, a character with a decimal value of 128 is displayed as `\x80`.
- This command is restricted to the file names that are obtainable from the `list` command. The `list` command displays the file names of all of the files that can be acted upon by certain commands. In addition to the `tail` command, the following commands can act upon the files that are listed with `list`:

`cat`

Display the contents of one or more files.

`delete`

Delete one or more files.

`more`

Display the contents of one or more files and pause at the end of each screen.

OPTIONS

`-f`

Follow the file as new text is added to it. The `tail -f` command prints the last 10 lines of the file but does not exit. As new text lines are added to the file, `tail` displays the new text lines. The `-f` option is useful for monitoring a log file as additional information is added to the log file. If you type `tail`

`-f log_name` and nothing seems to happen, the file is empty, the file is not being written to, or both.

To stop monitoring a file, press **Ctrl+C**.

`--help, -h`

Display this message.

ARGUMENTS

log_name

log_name can be any of the following:

- `agent_log`
- `battery.log`
- `bmclient_log`
- `bmserver_log`
- `boot.log`
- `BrightmailLog.log`
- `conduit_log`
- `cron`
- `db-migration.log`
- `dds.log`
- `dmesg`
- `imlinkage_log`
- `imrelay_log`
- `jlu-controller_log`
- `liveupdt.log`
- `maillog`
- `messages`
- `named.run`
- `secure`
- `update.log`

EXAMPLES

Example 1

Display the last 50 lines of the `BrightmailLog.log` log file.

```
tail BrightmailLog.log
```

Example 2

During an update, monitor the `update.log` log file. If you see information being written to `update.log` periodically, it usually means that the update is proceeding normally.

```
tail -f update.log
```

SEE ALSO

See [list](#) on page 51.

telnet

`telnet` – a standard Linux command to connect to a remote computer

DESCRIPTION

The `telnet` command lets you log into the command line of another computer on your network from the appliance.

Type `help telnet` on the command line for more information about the options available for `telnet`. The information that is displayed may contain references to commands that are not available on Symantec Messaging Gateway.

This command is a standard Linux command that has not been modified.

traceroute

`traceroute` – a standard Linux command to view the path taken by network packets

DESCRIPTION

The `traceroute` command displays the network route to the given hostname or IP address.

Type `help traceroute` on the command line for more information about the options available for `traceroute`. The information that is displayed may contain references to commands that are not available on Symantec Messaging Gateway.

This command is a standard Linux command that has not been modified.

update

`update` – update the appliance software

SYNOPSIS

```
update check | list
update [--version number] ( download | install | notes )
update --help
```

DESCRIPTION

You can perform the following tasks with the `update` command:

- Check for new software updates
- Download software updates
- Install software updates
- List the available software updates for download or installation

Before you update the software, ensure that your appliance does not perform any tasks that if disrupted could cause problems after you reset the system.

OPTIONS

`--help, -h`

Display this message.

`--version, -v`

Specify a software update version number for the `download`, `install`, or `notes` arguments. Use `update list` to determine what versions are available for the `--version` option.

ARGUMENTS

`check`

Perform a test update. The test update demonstrates what happens if you choose to perform a software update. Running `update check` does not update your appliance software.

download

Download but do not install a software update. After you download a software update, you can install it by typing `update install`. If you do not specify a version, the latest software update is downloaded.

If your Internet connection to the Symantec software update servers is not reliable, try downloading as a separate step from installing.

install

Download and install a software update. If you do not specify a version, the latest software update is installed on your appliance.

list

Display the available software updates.

notes

Display the software update notes. If you do not specify a version, the latest software update notes are displayed.

EXAMPLES

Download but do not install a software update. After you download a software update, you can install it by typing `update install`.

```
update download
```

SEE ALSO

